SAINT BEDE'S CATHOLIC HIGH SCHOOL

LYTHAM

ONLINE SAFETY POLICY

#March 2023

Please note within the lifetime of this policy there have been some personnel changes:

- Miss C Cochrane is Designated Safeguarding Lead (DSL)
- Mr R Gabrasadig is Deputy Headteacher (DHT)
- Miss Ashton has become Mrs D Taylor
- Safeguarding Governor is now Mr D Horton
- Ms Dickinson continues to be Online Safety Officer.

In addition, the previous BYOD Scheme has ceased and pupils do not bring their own devices into school. This section has been removed from the policy.

Development, Monitoring and Review of the Online Safety Policy

This online safety policy has been developed by the Senior Leadership Team and the Online Safety Officer. Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development, Monitoring and Review

This online safety policy was approved by the Governing Body on:	May 2023
The implementation of this online safety policy will be monitored by the:	Senior Leadership Team and the Online Safety Officer
Monitoring will take place at regular intervals:	Annually
The Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Annually
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	May 2024
Should serious online safety incidents take place, the following external persons and agencies should be informed as appropriate:	LA Safeguarding Officer, Children's Social Care, Police

The school will monitor the impact of the policy using:

- logs of reported incidents
- monitoring logs of internet activity (including sites visited)
- internal monitoring data for network activity
- surveys and questionnaires of
    - pupils
    - parents and carers
    - staff

Scope of the Policy

This policy applies to all members of the school community including staff, pupils, volunteers, parents and carers, visitors and community users who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but are linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body, Mr Damian Horton, has taken on the role of Online Safety. The role of the Online Safety Governor:

- regular meetings with the Online Safety Officer
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant governors committee meeting

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety is delegated to the Safeguarding Lead and the Online Safety Officer.
- The Headteacher and Deputy Headteacher are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. The Deputy Headteacher has the responsibility for line managing and supporting the Online Safety Officer.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Officer.

Online Safety Officer

- leads the online safety committee:
  Mr R Gabrasadig, Deputy Headteacher
  Miss D Taylor, Behaviour Manager
  Mr D Horton, Governor
  Ms L Dickinson, Online Safety Officer
- takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies and documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- liaises with the Behaviour Manager regarding behaviour issue connected to online safety and relevant sanctions
- consults the Headteacher and Deputy Headteacher regarding serious online safety issues and those requiring referral to external agencies
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets termly with the Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- attends relevant governors' committee meeting
- reports regularly to Senior Leadership Team

Network Manager and Technical Staff

The Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority Online Safety Policy / Guidance
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that s/he keeps up-to-date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network, internet, Virtual Learning Environment, remote access and email is regularly monitored in order that any misuse and/or attempted misuse can be reported to the Headteacher, Senior Leader and Online Safety Officer for investigation, action and sanction
- that monitoring software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Headteacher and/or Online Safety Officer for investigation, action and/or sanction
- all digital communications with pupils and parents and carers are on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the online safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities, where allowed, and implement current policies with regard to these devices
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Senior Lead for Safeguarding and Child Protection (DSL)
Should be trained in online safety issues and be aware of the potential for serious child protection and safeguarding issues to arise from:

- sharing of personal data
- access to illegal and/or inappropriate materials
- inappropriate online contact with adults and strangers
- potential or actual incidents of grooming
- online bullying

Online Safety Group
The Online Safety Group will meet termly to conduct its remit of reviewing and monitoring, as detailed below.

Members of the Online Safety Group will assist the Online Safety Officer with:

- the production, review and monitoring of the school online safety policy and related documents.
- the production, review and monitoring of the school filtering policy and requests for filtering changes.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network, internet and incident logs
- consulting stakeholders – including parents and carers and the pupils about the online safety provision
- monitoring identified improvement actions

Pupils

- Pupils are responsible for using the school's digital technology systems in accordance with the Pupil Acceptable Use Policy
- Pupils should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Pupils need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Pupils will be expected to know and understand policies on the use of mobile devices and digital cameras. Pupils should also know and understand policies on the taking and use of images and on online bullying.
- Pupils should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school if related to their membership of the school.

Parents and Carers
Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, the school website, the VLE and information about national and local online safety campaigns and literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website, VLE and online pupil records
- their children's personal devices in the school

Community Users
Community Users who access school systems, website, VLE as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems

Policy Statements

Education - Pupils
Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and is provided in the following ways:

- A planned online safety curriculum is be provided as part of Citizenship, Challenge Week, assemblies and other lessons and is regularly revisited.
- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial and pastoral activities.
- Pupils are taught in all lessons to be critically aware of the materials and content they access online and be guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils are helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff are to act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. The school filters make it highly unlikely that inappropriate material will become available, although it is recognised that no system can guaranteed one hundred percent results.

Education - Parents and Carers
Some parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's online behaviours. Parents and carers may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school seeks to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, website, VLE, social media sites
- Parents and carers sessions
- High profile events and campaigns
- Reference to the relevant websites and publications

Education & Training - Staff and Volunteers
It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training is be offered as follows:

- A planned programme of formal online safety training is made available to staff. This is regularly updated and reinforced. An audit of the online safety training needs of all staff is carried out regularly. It is expected that some staff will identify online safety as a training need within the performance management process.
- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Agreements.
- The Online Safety Officer receives regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff team meetings and/or INSET days.
- The Online Safety Officer will provide advice, guidance and training to individuals as required.

Training - Governors
Governors are invited to take part in online safety training and awareness sessions, with particular importance for those who are members of any sub-committee or group involved in technology, online safety, health and safety and child protection. This is offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation.
- Participation in school training and information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical - Infrastructure, equipment, filtering and monitoring
The school has an in-house managed ICT service working with two outside partners, who support the school in its provision of ICT services. The partners are Lancashire County Council/BTLS and Stone Computers

- School technical systems are managed in ways that ensure that the school meets recommended technical requirements
- There are on-going reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling are be securely located and physical access restricted
- All users have clearly defined access rights to school technical systems and devices.
- All users are provided with a username and secure password by a member of the network staff who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every ninety days.
- The administrator's passwords for the school ICT system, used by the Network Manager are kept in a secure place, known to the Headteacher.
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by BTLS/Lancashire County Council (Lightspeed) and Meraki
- The school provides enhanced, differentiated user-level filtering, allowing different filtering levels for different groups of users – staff, pupils etc.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement. The school users Impero software to monitor its own devices. Meraki and Lightspeed monitor other devices using the wired and wireless networks.
- An appropriate system is in place for users to report any actual or potential technical incident or security breach to the relevant person, as agreed). All staff and pupils are aware that any breach should be reported directly to the Network Team.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date virus software. BTLS/Stone/Meraki supply these services.
- An agreed policy is in place for the provision of temporary access of guests. All trainee teachers, supply teachers and other visitors onto the school systems receive a unique username and password.
- An agreed policy is in place (please see tables below) regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see School Personal Data Policy Template in the appendix for further detail)

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school informs and educates users about these risks and implements policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents and carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents and carers comment on any activities involving other pupils in the digital and video images. At each event, signage and announcements are in place.
- Staff and volunteers are allowed to take digital and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital and video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images in school unless they are used for educational purposes.
- Photographs published on the website, or elsewhere, that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or social media sites
- Pupil's work can only be published with the permission of the pupil and parents and carers.

Data Protection
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data. School is preparing to ensure compliance with GDPR (May 2018) and accessing support and training provided by the local authority

The school will ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out Find data RA template online
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage and cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office. Needs adding to AUP

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks, cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software

- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks and disadvantages:

	Staff and other adults				Pupils				
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed	Restrictions
Communication Technologies									
Mobile phones may be brought to school	X				X				Pupils - only to be used by pupil in social time to listen to music on the yard. Pupils - only to be used by pupils in lessons for educational purposes with permission from a member of staff.
Use of mobile phones in lessons		X					X		Staff - for professional purposes only. Pupils - Only to be used in lessons for educational purposes with permission from a member of staff.
Use of mobile phones in social time	X				X				Pupils - only to be used by pupil in social time to listen to music on the yard.
Taking photos on mobile phones, cameras, devices	X						X		Staff - for professional purposes only. Pupils - with permission from a member of staff for educational purposes only.
Use of other mobile devices e.g. tablets, gaming devices	X						X		Staff - for professional purposes only. Pupils - with permission from a member of staff for educational purposes only.
Use of personal email addresses in school, or on school network	X							X	Staff - during social time for personal communications only. Pupils - no.
Use of school email for personal emails				X				X	Staff - no. Pupils - no.
Use of messaging apps		X						X	Staff - during social time for personal communications only. Pupils - no.
Use of social media		X						X	Staff - during social time for personal communications only and in-line with school policy. Pupils - no.
Use of blogs	X						X		Staff - for professional purposes only Pupils - for educational purposes only.

When using communication technologies the school considers the following as good practice:

- The official school email service is regarded as safe and secure and is monitored. Users are aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access). Staff should ensure that all electronic communications with children and other adults are appropriate. Staff should use only the specified acceptable and permissible modes of communication, i.e. their school email/Office 365 account (@stbedeslytham.lancs.sch.uk) or the school's VLE (Firefly) to communicate with pupils and other adults.

- Users must immediately report, to the Online Safety Officer and/or Headteacher, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

- Any digital communication between staff and pupils or parents and carers (email, chat, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils are taught about online safety issues, such as the risks attached to the sharing of personal details. They are also taught strategies to deal with inappropriate communications and are reminded of the need to communicate appropriately when using digital technologies.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes this policy sets out clear guidance for staff to manage risk and behaviour online. Core messages include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. While, Ofsted's 'Online Safety Framework 2012', reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise.

The school and local authority have a duty of care to provide a safe learning environment for pupils and staff. School and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, online bully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents and carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes is checked regularly by the Online Safety Officer to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable and inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows in the table below:

Unsuitable and inappropriate activities

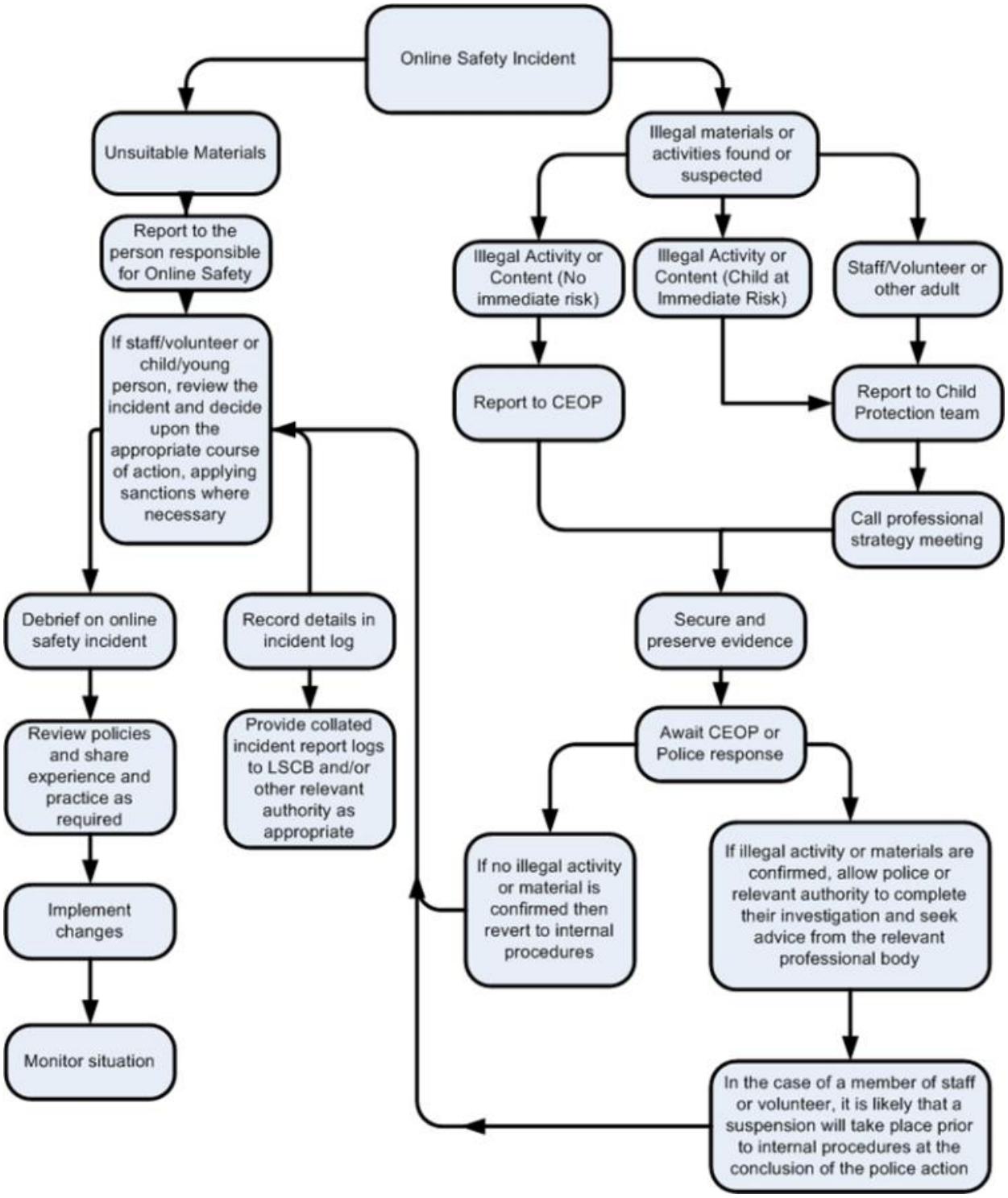
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make, posts, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	X
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
Online gaming (educational)		X				
Online gaming (non-educational)			X			
Online gambling					X	
Online shopping / commerce			X			
File sharing			X			

Use of social media			X Staff		
Use of messaging apps			X Staff		
Use of video broadcasting e.g. YouTube			X Staff		

Responding to incidents of misuse
This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above)

Illegal Incidents

If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated device/computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same device/computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national/local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials
- Isolate the device/computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes.

The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as detailed in the table below:

Pupils	**Actions / Sanctions**

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Online Safety Officer	Refer to Headteacher / DHT	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents and carers	Removal of network / internet access rights	Mark Behaviour Card	Warning	Further sanction/Refer to Behaviour Manager for e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			X	X	X	X	X				
Unauthorised use of non-educational sites during lessons	X										
Unauthorised use of mobile phone / digital camera / other mobile device during lessons	X										x
Unauthorised use of mobile phone / digital camera / other mobile device during social time											x
Unauthorised use of social media /messaging apps / personal email during lesson	X										x
Unauthorised use of social media /messaging apps / personal email during social time											x
Unauthorised downloading or uploading of files			X			X					X
Allowing others to access school network by sharing username and passwords			X			X					X
Attempting to access or accessing the school network, using another pupil's account			X			X	X				X
Attempting to access or accessing the school network, using the account of a member of staff			X			X	X				X
Corrupting or destroying the data of other users			X			X	X				X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X				X				X
Continued infringements of the above, following previous warnings or sanctions			X	X			X				X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X	X			X				X
Using proxy sites or other means to subvert the school's filtering system			X	X		X	X				X
Accidentally accessing offensive or pornographic material and failing to report the incident			X	X			X				X
Deliberately accessing or trying to access offensive or pornographic material			X	X			X				X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X	X			X				X

Staff **Actions / Sanctions**

Incidents:	Refer to line manager	Refer to Online Safety Officer	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			X	X	X				
Inappropriate personal use of the internet/social media /personal email		X	X						
Unauthorised downloading or uploading of files		X	X			X			
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X	X			X			
Careless use of personal data e.g. holding or transferring data in an insecure manner		X	X						
Deliberate actions to breach data protection or network security rules		X	X			X			
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X			X			
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X						
Using personal email, social networking, instant messaging, text messaging to carrying out digital communications with pupils		X	X						
Actions which could compromise the staff member's professional standing		X	X						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X						
Using proxy sites or other means to subvert the school's filtering system		X	X			X			
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X			X			
Deliberately accessing or trying to access offensive or pornographic material		X	X			X			
Breaching copyright or licensing regulations		X	X						
Continued infringements of the above, following previous warnings or sanctions		X	X						